AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your affiant, Matthew J. Schrauger, Special Agent with Homeland Security Investigations (HSI), being duly sworn, does depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Homeland Security Investigations (HSI) in Nogales, Arizona and have been so employed since May 2021. As such, I am an investigative law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516. Prior to joining HSI, I was employed as a Border Patrol Agent in Tucson, Arizona and since 2011.

2. As a Special Agent for HSI, I am responsible for investigating laws enumerated in Title 8, Title 18, and Title 21 of the United States Code. Included in my responsibilities are the investigation of illicit contraband-smuggling, including narcotics smuggling, across the United States border. In preparing to become a Special Agent, I attended the Basic Criminal Investigator and the HSI Special Agent training programs at the Federal Law Enforcement Training Center in Glynco, Georgia.

3. During my career in law enforcement, I have participated in multiple investigations involving illegal drugs, bulk cash smuggling, and weapons. During these investigations, I have been involved in seizures of cocaine, heroin, methamphetamine, fentanyl, and other illicit or controlled substances. I have assisted in the interrogation of

numerous subjects/defendants involved in and/or arrested for drug and narcotics violations. I also participated in several joint interagency federal and state investigations. In the course of these investigations, I conducted thorough background checks of targets, conducted physical surveillance, and monitored and reviewed recorded conversations of drug traffickers.

4. The statements contained in this affidavit are based on my experience and background as a law enforcement officer and, in part, on information provided by other law enforcement officers, records obtained by those officers and corresponding summaries. I am familiar with the information submitted in this affidavit. As this affidavit is submitted for a limited purpose, it does not recite all aspects of this investigation, but only sufficient information to establish probable cause in support of the issuance of this search warrant.

PURPOSE OF AFFIDAVIT

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, which is an electronic device, specifically a cellular telephone described as:

a. One (1) white, iPhone, (hereinafter **Target Device #1** or **TD #1**)

4. As further noted below, I submit that there is probable cause to believe that **TD #1** contains evidence, as more fully set forth in Attachment B, of the activities, which occurred during and in relation to the commission of violations of Title 21, United States Code, Section 841: Possession with Intent to Distribute Controlled Substances, and Title 21, United States Code, Section 846: Conspiracy to Distribute Controlled Substances.

Further, I submit there is probable cause to believe that **TD #1** also contains evidence, fruits and instrumentalities of these crimes as well as the identities of persons involved, as more fully described in this search warrant and the attachments. The applied for warrant is to authorize a forensic examination of **TD #1** as described in Attachment A for the purpose of identifying electronically stored data as described in Attachment B.

6. **TD #1** is currently in the custody of HSI, at the HSI Office in Rio Rico, Arizona. As further noted below, **TD #1** was seized after the arrest of Kaitlan Leann BRUMLEY on November 13, 2022, by Customs and Border Protection Officers and HSI Nogales Special Agents at the DeConcini Port of Entry. As such, HSI personnel-maintained custody of the cellphone in accordance with agency policy and procedure.

7. The requested warrant would authorize the forensic examination of **TD #1**, for the purpose of identifying electronically stored data to include: any telephone numbers, including but not limited to numbers called, numbers stored for speed dial, pager numbers, names and addresses, electronically stored voice and text messages, calling card numbers, text messages, photos, videos and/or identifying information that may be stored in the memory of **TD #1** for the items described in Attachment A (incorporated herein by reference).

BACKGROUND ON SMARTPHONES

8. Based upon my knowledge, training, and experience, as well as information related to me by law enforcement officers and others experienced in the forensic examination of electronic communication devices, I know that certain types of cellular

telephones referred to as "smartphones" (such as **TD #1**) generally offer more advanced computing ability and internet connectivity than standard cellular telephones. Provided that internet access has been purchased through an electronic communication service provider for a particular smartphone, a smartphone is capable of running complete operating system software, has full access to the internet and/or electronic mail (including file attachments), is capable of text and instant messaging, can create and edit documents created with computer software, is capable of storing large amounts of data, and can be interfaced with desktop and laptop computers.

9. As described in Attachment B hereto, this affidavit seeks permission to locate not only data files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes which individual(s) used the device as well as the purpose of their use. Additionally, this affidavit seeks information about the possible location of other evidence.

10. As described in Attachment B hereto, this affidavit also seeks permission to search and seize certain electronic records that might be stored within the device. Some of these electronic records might take the form of files, documents, or other data that are user generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

11. Although some of the records requested in this affidavit might be found in the form of user-generated documents (such as electronic format documents, picture, and movie files), electronic communication devices (such as **TD #1**) can contain other forms

of electronic evidence that are not user-generated. In particular, an electronic communication device may contain records of how it has been used and/or the person(s) who utilized the electronic communication device. Based upon my knowledge, training, experience, as well as information related to me by law enforcement officers and other persons involved in the forensic examination of electronic communication devices, I know that:

a. Data on electronic communication devices not currently associated with any file can provide evidence of a file that was once on the electronic communication device, but has since been deleted or edited, or of a deleted portion of a file;

b. Virtual memory paging systems can leave traces of information on an electronic communication device that can be used to determine what tasks and processes were recently in use;

c. Web browsers, e-mail programs, social media platforms, and chat programs store configuration information on the electronic communication devices that can reveal information such as online nicknames and passwords;

d. Operating systems can record additional information, such as the attachment of peripheral electronic devices, and the number of occasions in which the peripheral electronic devices were accessed;

e. Computer file systems can record information about the dates that files were created and the sequence in which they were created. This information may be evidence of

a crime and/or indicate the existence and/or location of evidence in other locations on the electronic communication device;

f. When an electronic communication device has more than one user, files can contain information indicating the dates and times that the files were created as well as the sequence in which the files were created, and whether a particular user accessed other information close in time to the file creation dates, times, and sequences;

g. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying an electronic communication device user, and contextual evidence excluding an electronic communication device user. All of these types of evidence may indicate ownership, knowledge, and intent to commit a given offense;

h. The foregoing type of evidence is not "data" that can be segregated, that is, this type of information cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how electronic communication devices operate and how electronic communication devices are used. Therefore, contextual information necessary to understand the evidence to be seized, as described in Attachment B also falls within the scope of the warrant.

CHARACTERISTICS OF INDIVIDUALS INVOLVED IN

DRUG TRAFFICKING ORGANIZATIONS

12. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the activities of drug smugglers and drug trafficking distribution networks. I became familiar with the manner in which drug traffickers smuggle, package, transport, store, and distribute drugs as well as how they collect and launder drug proceeds. I am also familiar with the manner in which drug traffickers use telephones, cellular telephone technology, internet, pagers, coded communications, and slang-filled conversations, false and fictitious identities and other means to facilitate their illegal activities and mislead law enforcement investigations.

13. Over the course of my experience in law enforcement, I learned that individuals involved in drug trafficking often:

a. use vehicles, typically containing secret compartments, as a means to distribute drugs and drug proceeds;

b. use the United States Postal Service as well as private courier services such as United Parcel Service ("UPS") as a means to distribute drugs and drug proceeds;

c. physically handle and count money after receiving it in exchange for drugs, thereby leaving residue traces of controlled substances on the money;

d. maintain, use or employ firearms and ammunition in connection with their drug trafficking activities;

e. drug couriers are often paid to transport the controlled substances;

f. drug couriers often use different navigational applications when transporting controlled substances;

g. drug coordinators often communicate with the drug couriers to track the progress of the trafficking activities;

h. maintain in secure locations over which they have control (e.g., stash houses) large amounts of currency to finance their ongoing illicit business;

i. attempt to conceal the true origins of the proceeds of unlawful activity by engaging in various money laundering techniques, e.g., by creating shell corporations; using the services of attorneys, bankers, and accountants; establishing "front" businesses; and purchasing and/or titling their assets in fictitious names, aliases or in the names of relatives, associates, or business entities, to avoid detection of these assets by law enforcement agencies; and, although these assets are in other names, traffickers actually own and continue to use these assets and exercise dominion and control over them;

j. use all the available features of electronic devices such as cellular telephones, including using third-party messaging applications such as WhatsApp or Facebook, to facilitate communication between and among criminal associates and to document their criminal activities, e.g., by sending messages about and taking photographs and video of drugs, bulk currency, firearms, and other involved persons, vehicles, and locations; often such electronic evidence will contain embedded metadata that reveals the dates, times, and locations (e.g., GPS coordinates) of criminal activity;

k. maintain in secure locations over which they have control (e.g., stash houses) drugs; paraphernalia; firearms; and drug proceeds, which proceeds include domestic and foreign currency, financial instruments such as money orders or cashier's checks, physical objects such as jewelry, vehicles, and electronics; and records relating to the purchase of these and other assets purchased with the proceeds of unlawful activity and/or as a means to conceal unlawful activity; and

l. maintain in secure locations over which they have control (e.g., stash houses) physical and electronic documents relating to the sale and distribution of drugs and drug proceeds, and related money laundering activities, with such documents including, but not being limited to, receipts, ledgers, tickets, books, financial records, bank and credit account records, wire transfer records, real estate records, identification documents, contact lists recording names, addresses and telephone numbers of criminal associates, photographs and videos, and vehicle title and registration documents.

PROBABLE CAUSE

14. On November 13, 2022, Kaitlan BRUMLEY entered the United States from the Republic of Mexico at the DeConcini Port of Entry in Nogales, Arizona via the vehicle lanes. BRUMLEY was the driver and registered owner of a 2006 Jeep Commander bearing Arizona license plate SGA23K. Diego MENDOZA-Demarbiuex was the passenger sitting in the front seat.

15. During a post-primary inspection, a Canine Enforcement Officer (deployed his Narcotics Human Detection Dog (NHDD) to conduct a canine sniff of BRUMLEY's

vehicle. The NHDD alerted to a trained odor emanating from the driver's side undercarriage of BRUMLEY's vehicle.

16. In the secondary inspection area, a Customs and Border Protection Officer (CBPO) asked BRUMLEY where they were coming from, to which BRUMLEY said "California" but quickly corrected herself and said Nogales, Sonora.

17. A CBPO asked BRUMLEY and MENDOZA if they visited anyone in Nogales, Sonora, Mexico. At the same time, BRUMLEY said "no one" and MENDOZA said "yes, a grandmother." BRUMLEY then raised her voice and stated, "we went to visit my grandmother."

18. BRUMLEY and MENDOZA told the CBPO they stayed in Mexico over the weekend, and they were heading to Tucson, Arizona. BRUMLEY told the CBPO she was the registered owner.

19. The CBPO received an oral, negative customs declaration that included narcotics, prescription drugs, or $10,000 or more in currency.

20. The vehicle was scanned by the Z-Portal, a non-intrusive X-ray, where a certified CBPO observed anomalies in the gas tank and front frame.

21. CBPOs observed missing bolts and screws along the gas tank of BRUMLEY's vehicle.

22. Upon further inspection, CBPOs discovered a non-factory compartment molded around the gas tank.

23. Inside the non-factory compartment, CBPOs could visually see multiple bags containing blue pills.

24. CBPOs inspected the anomalies by the front frame of BRUMLEY's vehicle and discovered a non-factory compartment. Inside the compartment CBPOs discovered more clear bags containing blue pills.

25. CBPOs seized a total of 238 packages containing suspected fentanyl pills. The suspected fentanyl pills weighed 31.86 kilograms. A sample blue pill was tested using a Rapid Response Kit and tested positive for the properties of fentanyl.

26. On November 15, 2022, samples of the suspected fentanyl were taken to Laboratory and Science Services (LSS) at the Mariposa Port of Entry for preliminary testing and the results were positive for the properties of fentanyl.

27. During a post-Miranda interview of BRUMLEY, she stated that she does not know anybody in Nogales, Sonora, Mexico. BRUMLEY stated both she and MENDOZA slept in BRUMLEY's vehicle over the entire weekend. BRUMLEY specifically stated that they did not stay in a hotel at all during their visit to Nogales, Sonora, Mexico. BRUMLEY stated she and MENDOZA were together the entire time.

28. BRUMLEY then stated she did stop by her grandmother's house but did not actually see her grandmother during the trip.

29. BRUMLEY stated that she is the registered owner of the Jeep Commander and paid approximately $1,500 USD for the vehicle a few months ago.

30. BRUMLEY stated she was with the vehicle the entire visit except on one occasion when she and MENDOZA went into an abandoned building.

31. During a post-Miranda interview of MENDOZA, he stated that they went to BRUMLEY's grandmother's house Nogales, Sonora, Mexico, but agreed to find a hotel nearby.

32. MENDOZA stated that BRUMLEY paid for the hotel.

33. MENDOZA stated that he remained at the hotel on Saturday November 12, 2022, all day while BRUMLEY went out and explored. MENDOZA stated that BRUMLEY did not return until approximately 9:00 PM.

34. MENDOZA stated that they physically saw BRUMLEY's grandmother during their trip.

35. **TD #1** was receiving alerts during the interview. Multiple notifications in multiple text applications were identified. Also, multiple missed phone calls were identified. It is common in my training and experience that coconspirators will repeatedly contact the driver of a load of narcotics around the time a load driver is crossing the border. This is done to both check on if the load of narcotics was successfully smuggled across the border and to coordinate a meeting where the narcotics can be offloaded. A search warrant would allow agents to further examine these incoming messages and calls to potentially identify coconspirators and locations being used to offload or transfer narcotics.

36. Record checks performed on BRUMLEY revealed she is a citizen of the United States. BRUMLEY has only two other border crossings. Those occurred on October 16, 2022, and October 3, 2022.

37. **TD #1** was in BRUMLEY's possession when she was apprehended

38. Based on my training and experience, I know that drug traffickers use cellular devices to communicate and coordinate the distribution of narcotics for traffickers.

39. Since the date of the arrest, **TD #1** has been stored in a secure evidence location within HSI-Nogales. **TD #1** has been stored in such a manner that its contents, to the best of my knowledge, are in substantially the same state as when they first came into possession of HSI.

TECHNICAL TERMS

40. Wireless telephone: A wireless telephone (or mobile telephone or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates,

appointments and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

41. Digital camera: A digital camera is a camera that records pictures and video as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos. Most cell phones currently manufactured contain digital cameras as a standard feature.

42. Portable media player. A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock or games. Most cell phones currently manufactured contain portable medial players as a standard feature.

43. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state. Most cell phones currently manufactured allow the use of the Internet as a standard feature. Further, most current cell phones allow the user to transmit electronic messages via standard email services or specially designed communication applications between parties.

44. Based on my training, experience, research, and from consulting the manufacturer's advertisements and product technical specifications available online for these types of cellular phones, and based upon my discussions with experts, I know that the cellular phones which are the subject of this search warrant application most likely have capabilities that allow them to also serve as a radio communication transmitter, wireless telephone, GPS device, wireless internet connectivity, and text message capabilities, as these are generally standard features. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device; evidence of where such persons were when they possessed or used the device; evidence of who such persons were with when they possessed or used the device; evidence of persons with whom they communicated when they possessed or used the device; evidence of text, email, other electronic messaging applications and voice mail communications between the person who possessed or used

the device and others. Navigational coordinates may also be transmitted to and/or from these devices to determine the user's location through a GPS application.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

45. Based on my knowledge, training and experience, I know that electronic devices such as **TD #1** in this case, can store information for long periods of time. Similarly, things that have been viewed via or uploaded to the Internet are typically stored for some period of time on the device. Additionally, computer files or remnants of such files can be recovered even if they have been deleted. This is because when a person "deletes" the information on an electronic device, the data does not actually disappear, rather, the data remains on the storage medium until it is overwritten by new data. Information described in this affidavit can often be recovered by forensic computer experts using forensic tools and software.

46. As further described in this affidavit and Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how **TD #1** was used, where they were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on **TD #1** are more fully set forth in the factual section contained herein and because:

A. Data on the storage medium can provide evidence of a file that was once on thestorage medium but has since been deleted or edited, or of a deleted portion of a file, including frequency channels, text messages, video, or photographs.

B. Forensic evidence on a device can also indicate who has used or controlled the devices. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

C. A person with appropriate familiarity of how an electronic device works may, after examining the forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

E. Further, in finding evidence of how a device was used, the purpose of its use, who used it, when and where, sometimes it is necessary to establish that a particular thing is not present on a storage medium, for example, the absence of the entry of a name in a contact list as evidence that the user(s) of **TD #1** did not have a relationship with the party.

28. The examination of **TD #1** may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is

evidence described by the warrant. Because this warrant only seeks permission to examine a device already in the possession of HSI, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, there is probable cause for the Court to authorize execution of the warrant at any time in the day or night. Due to the nature of such cell phones, data contained within will remain uncorrupted when being stored for an extended period of time.

CONCLUSION

Based on the information listed above, I submit that there is probable cause to believe that URIAS-VIRREY has committed violations of criminal statutes including, but not limited to, possession with the intent to distribute controlled substances, in violation of 21 U.S.C. §§ 841(a)(1). Also, I believe evidence, fruits and instrumentalities of the foregoing violations, as particularly described in Attachment B, can be found in **TD #1**, which is particularly described in Attachment A.

Wherefore, I respectfully request that a warrant be issued authorizing any authorized law enforcement officer to enter and search the devices described in Attachment A for the items listed in Attachment B.

I swear under penalty of perjury that the foregoing is true and correct to the best of my information and belief.

MATTHEW J SCHRAUGER

Digitally signed by MATTHEW J SCHRAUGER
Date: 2022.12.21 18:36:19 -07'00'

Matthew J. Schrauger, Special Agent
Homeland Security Investigations

Subscribed and sworn telephonically this 21st day of December, 2022.

Eric J. Markovich,

Honorable ~~Thomas D. Ferraro~~
United States Magistrate Judge